What is claimed is;

1. An encryption control apparatus, comprising:

a CPU for running a program;

a ROM for storing the program run by the CPU;

a RAM used as a work area while the CPU is running the program;

an I/O section for sending/receiving data to/from an external device; and

an encryption section for decrypting encrypted data and encrypting plain text data,

wherein each of the foregoing components is formed on a single semiconductor device.

2. The encryption control apparatus according to claim 1, wherein:

the RAM stores a private key used in decrypting the encrypted data;

the ROM stores data specifying a party having an authorization to use the encryption control apparatus; and

the encryption control apparatus has a standby mode for waiting for data to be received from an external and an enable mode for enabling an operation, and further comprises mode switching means for decrypting encrypted data sent from the external in the standby mode with the private key stored in the RAM so that the plain text data is restored, the switching means also checking whether the plain text data coincides with the data stored in the ROM, and switching the encryption control apparatus to the enable mode or back to the standby mode

depending on coincidence and discrepancy of the data.

3. The encryption control apparatus according to claim 2, wherein:

the ROM stores a plurality of main programs run in the enable mode; and

the encryption control apparatus further comprises main program selecting means for selecting one of the plurality of main programs run in the enable mode based on the data sent from the external in the standby mode.

4. The encryption control apparatus according to claim 1, further comprising an authentication section, formed on the single semiconductor device, for sending/receiving data to/from an external information processing device that carries out information processing based on data sent/received to/from the encryption control apparatus, the authentication section also authenticating a data sender party to judge whether the data sender party is an authorized party.

5. The encryption control apparatus according to claim 1, further comprising key generating means for generating a key used in encrypting and decrypting data, so that the encryption control apparatus encrypts and decrypts the data with the key generated by the key generating means.

6. The encryption control apparatus according to claim 5, wherein the key generating means generates a private key and a public key, and sends the public key alone to an external and stores the private key in the RAM.

7. The encryption control apparatus according to claim

4, wherein:

the RAM stores a private key used in decrypting the encrypted data;

the ROM stores data for specifying a party having an authorization to use the encryption control apparatus; and

the encryption control apparatus further comprises I/O section control means for decrypting the encrypted data received in the authentication section with the private key stored in the RAM so that plain text data is restored, the I/O section control means also checking whether the plain text data coincides with the data stored in the ROM, and enabling the I/O section only when coincidence of the data is confirmed.

8. The encryption control apparatus according to claim 7, wherein:

the single semiconductor device includes a plurality of the I/O sections mounted thereon; and

the I/O section control means enables an I/O section corresponding to the data received by the authentication section based on the authentication data.

9. The encryption control apparatus according to claim 7, wherein:

the I/O section is allowed to be set to an arbitrary security level among a plurality of security levels; and

the I/O section control means sets the I/O section to a security level corresponding to the data received in the authentication section based on the data.

10. The encryption control apparatus according to claim

4, wherein the authentication section sends/receives the data to/from the external information processing device through a modem.

11. The encryption control apparatus according to claim 1, further comprising data destroying means for, upon receipt of abnormality detection, destroying a key stored in the RAM.